Authentication goals for MicroSan protocol

Utilize authentication to prevent accidental or various levels of malicious packet corruption.

1. Reject unauthorized clients based on MAC, Key, LBA & or IP address.
2. Invalidate clients based on history of unauthorized access attempts.
3. Reject Spoofed Client MAC or source IP packets w/o rejecting valid packets from valid clients.
4. Reject spoofed source IP
5. Minimize CPU cycles needed for authorization of sequential packets.
6. Authorize multiple out of order packets in flight within an adjustable window.
7. Provide a secure mechanism by which authorization windows are synchronized.
8. Provide a secure mechanism by which client owners can share authorization Keys.
9. Provide a secure mechanism by which MicroSan can share authorization Keys with client owner.
10. Provide a secure mechanism by which Client can manage MicroSan Partitions.
11. Provide a secure mechanism by which Client can authorize update of MicroSan Code & Features
12. Maximize the use of background processing of authorization headers.
13. Allow multiple clients simultaneous access to partitions.
14. Do not provide NAK for authentication failures.
15. Limit protection to header so as not to be covered by NSA algorithm restrictions.
16. Limit protection to authentication and not encryption. (LBA may be exception)
17. Prevent accidental or malicious data corruption by intervening routers & bridges.

Authentication proposal

In order to prevent accidental or various levels of malicious data corruption, ALL MicroSan support the following levels of packet authentication. The flexibility of these security levels is further enhanced by the ability of the client to choose between H/W MAC, Source IP and Rotating Keys of varying lengths. The described flexibility of these security levels addresses the widest possible range of data integrity and packet processing overhead...

Level	Key	MAC or IP	DAC	Encrypt LBA
0	None	None	None	None
1	None	Validate	Option	Option
2	Rotate	None	Option	Option
3	Rotate	Validate	Option	Option
4	Rotate	Option	Validate	Option
5	Rotate	Option	Validate	Encrypt

Level 0

Level 0 accepts any request from any client.

Level 1

Level 1 uses MAC or source IP to reject accidental or malicious packets from clients with MAC or source IP which do not match that of the device which created the partition. The MAC validation provides a significant level of hardware protection from virus spoofing of the source within the NIC but limit's access to the creating clients MAC address. The Source IP validation provides arguably less virus protection but allows for simpler sharing of partitions in an IP environment. Note that third parties could provide secure methods of changing their MAC address to allow a lost device to be replaced by the manufacturer.

Level 2

Level 2 uses rotating keys to reject accidental or malicious packets from clients who do not have the synchronization seed for the rotating key. The rotating key is of a special class of keys which allow the receiver of the packets to provide a variable window of valid rotating packet keys. Once used no packet key may be used again within a single synchronization. Rotation of the keys within the sliding window occurs as each packet is acknowledged or timed out. The window nature of this schema addresses IP's unique variable time-of-flight and out of order packet flexibility. Synchronization of the receivers rotating key window is maintained as an average moving window where the valid packets received are used to calculate the position of the receivers window.

The use of systolic processing of the packet keys allows the client to control the length of the key and therefore the maximum instantaneous processing burden required to authenticate packet keys. Authentication is further accelerated by using the Packet LBA to index into a much smaller group of keys within the sliding window.

Level 2 Rotating Key packet validation provides arguably greater virus protection than Level 0 or Level 1 while at the same time providing greater flexibility to share data among clients. It also addresses the special case security issues encountered in multicast packets.

New windows are created each time a client with a unique MAC or IP performs a synchronization. Each unique authorization window can be configured independently including: window size, time-of-life and key length. Unused windows are released when they remain unused beyond their time-of-life. It should be noted that multicast receivers will each have their own window but that the parameters of the window will be identical among all members of the multicast.

Optimally the rotating Key would be placed at the end of the packet so that all data is guaranteed to have been received before the valid key. This prevents malicious or accidental corruption of the data within a valid packet sent by a valid client.

Level 3

Level 3 uses rotating key and H/W MAC to reject accidental or malicious packets from clients who do not have the synchronization seed for the rotating key ***and*** are not the originating client hardware.

Level 3 Rotating Key with the added H/W MAC packet validation provides arguably the greatest protection from accidental and or malicious access to the MicroSan. The added level of security over Level 2 comes at the cost of sharing access among multiple clients. This level of security is envisioned primarily for high security access between the MicroSan and the client who created the partition. Which itself might be another MicroSan.

Level 4 (Optional)

Level 6 adds Data Authentication Coding to Levels (0-3) of the transport mechanism to allow the receiver verify that the LBA and data have not been accidentally or maliciously modified in the process of transport. It is envisioned that we would specify the use of the existing royalty free DAC or HDAC algorithms approved by the GSA and NSA.

Level 5 (Optional)

Level 5 adds encryption of the LBA to Level (0-4). LBA are encrypted using the same protocol and algorithm as Level 3 & 4. Encrypting the LBA denies potential malicious clients from snooping LBA histograms to help them focus their attack on sensitive areas of the partition such as file system directories (FAT TABLES). The LBA are encrypted using a different key and algorithm than that used for the rotating authorization key. Using different algorithms, seeds and keys prevents malicious clients from statistically decoding the authorization key using known LBA access patterns.

Great news for our authentication protocol...

The feds have a 5yr old ruling allowing "Strong" encryption of transport mechanisms so long as the mechanism can not be used to transfer data between devices over the public infrastructure... There is also a recent ruling declaring once and for all that IP is when 1: leaves a building or is broadcast on radio waves... they stopped short of specifically limiting light wave communication that leaves a premise...
Essentially these rulings allow Zetera to use existing public authentication algorithm that are accepted as being stronger that is allowed if you secure your transactions by encrypting the entire packet including the data. It is the data portion that is limited to 128 bits by the ruling. Our transport header based authentication hides NO user data and is therefore exempt from the DES, AES and 128 bit mandates for exchange of information on the public infrastructure.
What this means is that we will probably allow clients to use authentication seeds up to 1024 bytes that are up to 8192 bits long... This forces an attacker to perform 2^32 Billion math operations within the time-of-life of the moving window...
Since the time-of-life of a given key window will probably be limited to a maximum of 500ms an attacker would be forced to successfully crack the key within 500ms to create spoofed keys that would be accepted by the device receiving the packet. The short window also prevents the use of massively networked arrays of computers since they can not trade more than a few hundred packets between them within the 500ms latency window.
It is also a reasonable argument to exclude the LBA of the data as being restricted as data since it carries only "Transport" information on "How" to store the data not Data to be stored... This will allow us to use strong variable length encryption on the LBA to deny attackers information on the workings of the transport and storage protocols... This still meets with the NSA requirements that they be able to DECODE the transported data since the data portion of the packet will be supplied by the device and hence be restricted to using "Approved" encryption technologies.
- Tom